Quality - Security uncompromised and Plausible Watermarking for Patent Infringement

Yamuna Govindarajan yamunaphd@yahoo.com
Reader /Department of Electrical and Electronics Engg
Annamalai University
Annamalai Nagar -608002,India

Sivakumar Dakshinamurthi
Professor / Department of Electronics and Instrumentation Engg dsk2k5@gmail.com
Annamalai University
Annamalai Nagar -608002,India

Abstract

The most quoted applications for digital watermarking is in the context of copyright-protection of digital (multi-)media. In this paper we offer a new digital watermarking technique, which pledges both Security and Quality for the image for the Patent protection. This methodology uses tale techniques like Shuffling, Composition & Decomposition, and Encryption & Decryption to record the information of a protected primary image and the allied watermarks. The quadtree can aid the processing of watermark and AES provides added security to information. Besides that, we intend a novel architecture for Patent Protection that holds promise for a better compromise between practicality and security for emerging digital rights management application. Security solutions must seize a suspicious version of the application-dependent restrictions and competing objectives.

Keywords: Digital watermarking, Patent protection, Shuffling, Quadtree, Advanced Encryption Standard.

1. INTRODUCTION

Digital watermarking is a technique which allows an individual to add hidden Patent notices or other verification messages to digital audio, video, or image signals and documents. Such a message is a group of bits describing information pertaining to the signal or to the author of the signal (name, place, etc.). The technique takes its name from watermarking of the paper or money as a security measure [1]. According to the human perception, the digital watermarks can be divided into two different types as follows: visible and invisible. Visible watermarks change the signal altogether such that the watermarked signal is totally different from the actual signal, e.g., adding an image as a watermark to another image. Invisible watermarks do not change the signal to a perceptually great extent, i.e., there are only minor variations in the output signal. An example of an invisible watermark is when some bits are added to an image modifying only its least significant bits (LSB).

Patent protection for multimedia information has been a key concern of multimedia industry. The electronic representation and transfer of digitized multimedia information (text, video, and audio)

have increased the potential for misuse and theft of such information, and significantly increases the problems associated with enforcing Patents on multimedia information. Digital watermarking technology opens a new door to authors, producers, publishers, and service providers for protecting their rights and interests in multimedia documents [2].

In order to protect the patent of a digital image, a matured digital image watermarking technique must have to meet the following properties [3]:

- Perceptual transparency: The algorithm must embed data without affecting the perceptual quality of the underlying host signal.
- Security: A secure data embedding procedure cannot be broken unless the unauthorized user access to a secret key that controls the insertion of the data in the host signal.
- Robustness: The digital watermark must survive after being attacked by lossy data compression and image manipulation and processing operations, e.g. cut and paste, filtering, etc.
- Unambiguous: Retrieval of the watermark should unambiguously identify the owner.
- Universal: The same watermarking algorithm should be applicable to all multimedia under consideration.
- Imperceptibility: The watermark itself should not be visible by the human visual system (HVS) and should not degrade the image quality.
- Reliability: To ensure that the project application returns the correct watermark each time. In spite of the loss of watermarking information by the optimizer, we should always be able to obtain correct and accurate results from the project.

Today two technologies are applied when protecting image data in Digital Rights Management (DRM) environments: Encryption and Digital watermarking. Encryption renders the data unreadable for those not in the possession of a key enabling decryption. This is especially of interest for access control, as usage of the image data is restricted to those owning a key.

Digital watermarking adds additional information into an image file without influencing quality of file size. This additional information can be used for inserting Patent information or a customer identity into the image file. The latter method is of special interest for DRM as it is the only protection mechanism enabling tracing illegal usage to a certain customer even after the image data has escaped the secure DRM environment.

In general these two mechanisms show a certain antagonism with respect to the transparency requirements of the encrypted, respectively watermarked data. Both mechanisms apply small media type specific changes on the cover data. But whereas transparent watermark embedding should keep the auditory quality of the marked data unaffected, partial encryption is targeted on maximum effect on the quality of the digital media

1.1 Related Work

Rahul Shukla, Pier Luigi Dragotti, Minh Do_, and Martin Vetterli [5] have proposed a novel coding algorithm based on the tree structured segmentation, which achieves the oracle like exponentially decaying rate-distortion (R-D) behavior for a simple class of signals, namely piecewise polynomials in the high bit rate regime. Raphael Finkel and J.L.Bentley have proposed [6] an

optimized tree and an algorithm to accomplish optimization in *n* log *n* time. They discuss the specific case of two-dimensional retrieval, although the structure is easily generalized to arbitrary dimensions. P. Strobach proposes [7] the concept of recursive plane decomposition (RPD) is embedded in a quadtree data structure to obtain a new variable block size image coding algorithm that offers a high performance at a low computational cost.

H. K. C. Chang, P. M. Chen, and L. L. Cheng have proposed [10] an efficient data structure, called the common-component binary tree (CCBT), to hold the linear quadtrees corresponding to a set of similar binary images. T. W. Lin has come out with [11] a new approach for storing a sequence of similar binary images Based on linear quadtree structures and overlapping concepts. F. Boland, J. O. Ruanaidh, and C. Dautzenberg have proposed[12] an overview of watermarking techniques and a solution to one of the key problems in image watermarking, namely how to hide robust invisible labels inside grey scale or colour digital images. Ji-Hong Chang and Long-Wen Chang have proposed [13] a new digital watermarking algorithm for images with bar code and digital signature and their simulation shows that the proposed algorithm gets satisfactory results for various attacks. Hans Georg Schaathun have proposed[14] to prevent un authorised copying of copyrighted material, by tracing at least one guilty user when illegal copies appear and they describe how error-correction makes it possible to relax this assumption, and they modify two existing schemes to enable error-correction. Soroosh Rezazadeh, and Mehran Yazdi [15] have discussed a robust digital image watermarking scheme for copyright protection applications using the singular value decomposition (SVD).

JUAN R. HERNA´ NDEZ, FERNANDO PE´REZ-GONZA´ LEZ have found [16] a statistical approach to obtain models that can serve as a basis for the application of the decision theory to the design of efficient detector structures. M. Barnia, F. Bartolinib, V. Cappellinib, E. Maglic, G. Olmo have conversed [17] near-lossless digital watermarking for copyright protection of remote sensing images and they show that, by forcing a maximum absolute difference between the original and watermarked scene, the near-lossless paradigm makes it possible to decrease the effect of watermarking on remote sensing applications to be carried out on the images. Md. Mahfuzur Rahman and Koichi Harada have proposed [18] a parity enhanced topology based spot area watermarking method to embed information in objects with layered 3D triangular meshes such as those reconstructed from CT or MRI data.

Nizar Sakr, Nicolas Georganas, and Jiying Zhao have proposed [19] an adaptive watermarking algorithm which exploits a biorthogonal wavelets-based human visual system (HVS) and a Fuzzy Inference System (FIS) to protect the copyright of images in learning object repositories. Jacob Löfvenberg, Niclas Wiberg have mentioned [20] the performance of random fingerprinting in conjunction with a specific testing method.

1.2 Objective of the Work

In our paper, We propose a new algorithm which for Patent Protection which will neither affect the quality of the Patent Image, nor compromise the security also.

This method is to shuffle the digital watermark into a primary image, then projected on to the spatial domain, combined with the information of digital watermark and primary image, and creates a Patent secret code vector (PSCV). This PSCV can be authorized and becomes a critical message for the future image patent argument. When certification authority generates the 256 bit secret key, Encrypted PSCV and argued image will extract watermark from the image for the purpose of image patent loyalty judgment. In our method, the primary image will not be modified nor created watermarked image. The proposed technique is suitable for non-modifiable image; for instance, medical image. This paper is composed of following sections: Section 2 details the proposed methodology, Section 2.1 briefly introduces Shuffling and Projection Technique, Section 2.2 briefs quadtree structure, Section 2.3 briefs Encryption technique. Section 3 demonstrates the experimental results and the discussions. Finally, the conclusions are presented in Section 4.

2. THE PROPOSED METHODOLOGY

Patent protection has become a hot issue in current digitized world due to the prevailing usage of Internet and an accumulation of multimedia data distribution, for instance, audio, image, and video. Digital watermarking techniques can protect images intellectual property right efficiently. We are proposing a new digital watermarking technique for the Patent protection. Figure: 1 represents the Block Diagram of the proposed methodology. The technique is discussed in 2.1, also Shuffling technique, Quadtree, AES algorithm is discussed in 2.2, 2.3, and 2.4 respectively.

2.1 The Algorithm

2.1.1 Generation of Patent Secured Secret Code Vector (SSCV)

Input: Primary Image (I_p), Patent Image(I_c), Key seed (K_s)

Sp ← Size of (I_p)

Sc ← Size of (I_c)

1. First the I_c is shuffled to get Shuffled Image (I_s) of size S_c
2. A key(K_u) is generated from a random number using K_s
3. Arrive X position (XI_y) , Y Position (YI_y) from K_u
4. Based on the position XI_y, YI_y a new image is yielded from the I_p , called sub primary image/Yielded Image (I_y)
5. I_s is projected on I_y to arrive projected image I_{pr}
6. I_{pr} is decomposed to get the Patent Secret Code Vector (PSCV)
7. Generate 256 bit key (A_k) from the random seed Ks
8. Encrypt the PSCV using the key A_k to get the SSCV

2.1.2. Generation of Patent Image / Watermark Image (Ic)

1. Input: SSCV, I_p, K_s
2. Generate 256 bit key (A_k) from the random seed K_s
3. SSCV is decrypted using (A_k) to get PSCV
4. PSCV is composed to get I_{pr}
5. A key(K_u) is generated from a random number using K_s
6. Arrive X position (XI_y) , Y Position (YI_y) from K_u
7. Based on the position XI_y, YI_y a new image is yielded from the primary image (I_p).
8. I_y is projected on Ipr to arrive I_s
9. Is will be reshuffled to get I_c which is Patent image

2.1.3. Verification Process

1. The Secured Secret Code Vector of the user ($SSCV_u$) is claimed to get an image I_{cu}.
2. Compare the Claimed Image I_{cu} with the Patent Image I_c.
3. If I_{cu} and Ic are equal, then claimed user is the Owner of the Patent Image, besides the claimed user is not the owner of the Patent image.

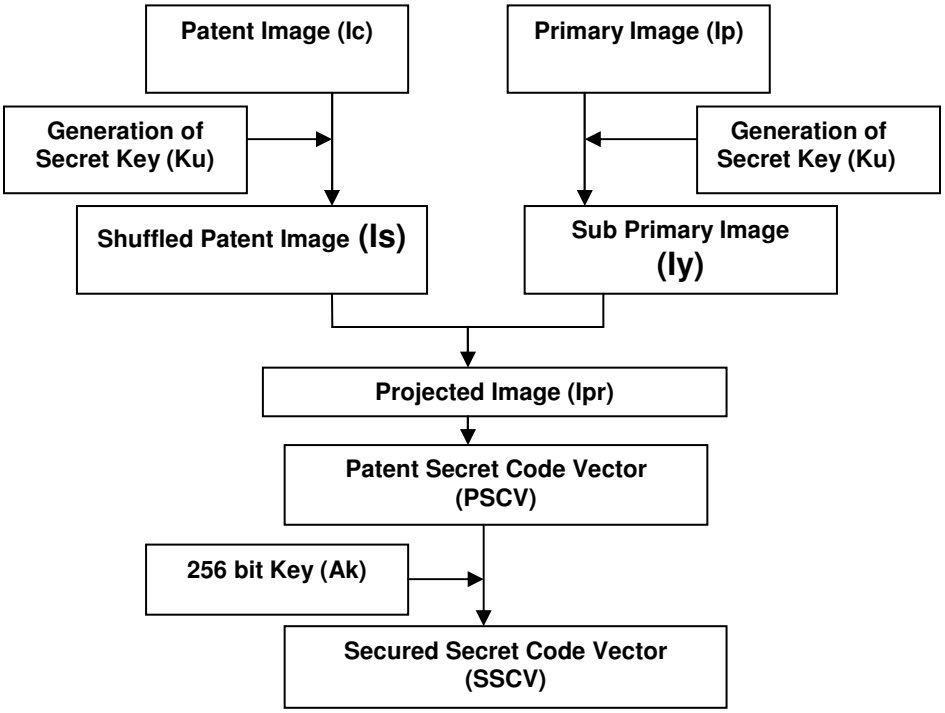


FIGURE: 1 Block diagram of the proposed methodology

2.2 Shuffling and Projection Technique

Shuffling is a linear-time algorithm (as opposed to the previous O(n log n) algorithm if using efficient sorting such as merge sort or heap sort) which involves moving through the pack from top to bottom, swapping each in turn with another from a random position in the part of the pack that has not yet been passed through (including itself). Providing that the random numbers are unbiased, this will always generate a random permutation [4].

2.2.1. Shuffling Technique

We have proposed a Shuffling methodology here. I_{cv} is the Vector representation of copyright image .The locations for the shuffled image(S_L) is generated as follows:

$$S_L=\{ x_i : p(x_i) , x_i \notin \{xk\}, i=0,..N-1,k=0,. i-1\} \quad (1)$$

Where N is size of Copyright image

$$p(x_i) = \text{mod } (PRNG(r_s) , N) , \ i=0 , \dots , N-1 \quad (2)$$

$$SI_{vi} = \{ y_i : p(y_i) , i=0,..N-1) \quad (3)$$

$$p(y_i) = I_{cv}[S_L[i]] \qquad i=0,\dots N-1 \quad (4)$$

The shuffled image is then reconstructed from the shuffled vector and is represented as I_s, Where PRNG is the pseudo random number generation function.

SI_v is the Shuffled Image Vector. rs is the seed value for PRNG and is defined as follows

$$rs_n = r_{n-1}, \ n=1,\dots N-1 \quad (5)$$

When n =0, rs_0 = key seed value
SI_v is converted to sqrt(N) x sqrt(N) matrix which is I_s (Shuffled Patent Image).

2.2.2. Projection Technique

During Composition I_s^T is projected on $(I_y^T)^{-1}$ to get Ipr

$$I_{pr} = (I_s^T * (I_y^T)^{-1}) \quad (6)$$

During Decomposition I_y is projected on I_{pr}^T to retrieve I_s

$$I_s = I_y * I_{pr}^T \quad (7)$$

2.3. Quad Tree

A quadtree is a tree data structure in which each internal node has up to four children. Quadtrees are most often used to partition a two dimensional space by recursively subdividing it into four quadrants or regions. The regions may be square or rectangular, or may have arbitrary shapes. A node of a point quadtree is similar to a node of a binary tree, with the major difference being that it has four pointers (one for each quadrant) instead of two ("left" and "right") as in an ordinary binary tree. Also a key is usually decomposed into two parts, referring to x and y coordinates. Therefore a node contains following information:

- 4 Pointers: quad['NW'], quad['NE'], quad['SW'], and quad['SE']
- point; which in turn contains: key; usually expressed as x, y coordinates

The leaf node in the quadtree represents a quadrant with identical pixels. The color of the leaf node is the same as its corresponding quadrant. On the other hand, the internal node represents a quadrant mixed by black pixels and white pixels. The quadrant corresponding to an internal node is still needed to be recursively subdivided [5, 6, 7].

2.4. Advanced Encryption Standard

Encryption renders the data unreadable for those not in the possession of a key enabling decryption. This is especially of interest for access control, as usage of the image data is restricted to those owning a key. For this Encryption we use an AES algorithm, which is more secured compare to DES. AES supports key sizes of 128 bits, 192 bits and 256 bits and will serve as a replacement for the Data Encryption Standard which has a key size of 56 bits.

AES stands for Advanced Encryption Standard. AES is a symmetric key encryption technique which will replace the commonly used Data Encryption Standard (DES). AES is secure enough to protect classified information up to the TOP SECRET level, which is the highest security level and defined as information which would cause "exceptionally grave damage" to national security if disclosed to the public [8].

In addition to the increased security that comes with larger key sizes, AES can encrypt data much faster than Triple-DES, a DES enhancement that which essentially encrypts a message or document three times. According to NIST's "The AES algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information"[9]. Table 1 compares the advantages of AES with DES

3. EXPERIMENTAL RESULTS AND DISCUSSION

In our experiments, for a given grey-valued primary image I_p, its image size is 512 x 512 pixels. In that, there is a 64 x 64 grey Patent image I_c which is to be shuffled to get the shuffled image Is. First, in our method, a secret key K_u is chosen. The Patent is shuffled by using Random number seed (Ks) to select 64 x 64 permuted coordinates. Then, a sub primary image/yielded image Iy with 64 x 64 pixels is selected from "Barbara" by applying Ks to get the top-left coordinate of Iy in Ip. The next step is to generate a projected image Ipr for Iy and Is. The algorithm then recursively divides each Ipr image into equal size quadrants, respectively. A secret code vector PSCV is built by using a quadtree decomposer. Besides that we do Encryption by using AES algorithm which is more secured in that a 256 bit key Ak is used to get the Secured secret code vector SSCV. The watermark process is finished after the SSCV is built. Finally, the recovered watermark image is obtained by reversal of the above process. Figure 2 are sample images of PSCV Construction and Figure 3 are example of reconstruction.

Table 1: Comparing DES and AES

	DES	AES
Key Length	56 bits	128, 192, or 256 bits
Cipher Type	Symmetric block cipher	Symmetric block cipher
Block Size	64 bits	128, 192, or 256 bits
Developed	1977	2000
Cryptanalysis resistance	Vulnerable to differential and linear cryptanalysis; weak substitution tables	Strong against differential, truncated differential, linear, interpolation and Square attacks
Security	Proven inadequate	Considered secure
Possible Keys	2^{56}	2^{128}, 2^{192}, or 2^{256}
Possible ASCII printable character keys*	95^{7}	95^{16}, 95^{24}, or 95^{32}
Time required to check all possible keys at 50 billion keys per second**	For a 56-bit key: 400 days	For a 128-bit key: 5 x 10^{21} years

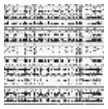
* When a text password input by a user is used for encryption (there are 95 printable characters in ASCII).

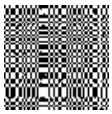
**In theory, the key may be found after checking 1/2 of the key space. The time shown is 100% of the key space.

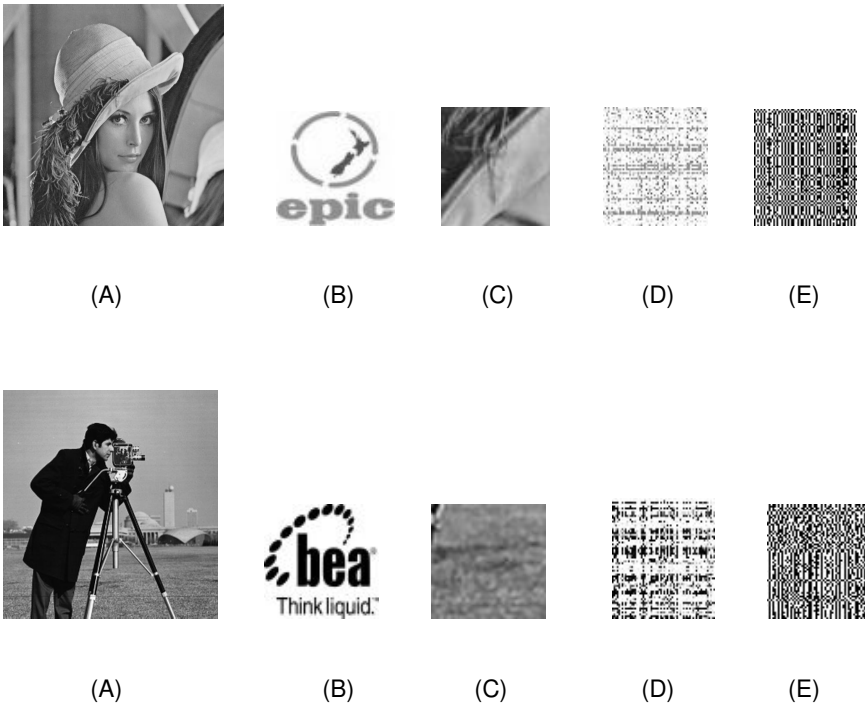

(A)

(B)


(C)


(D)

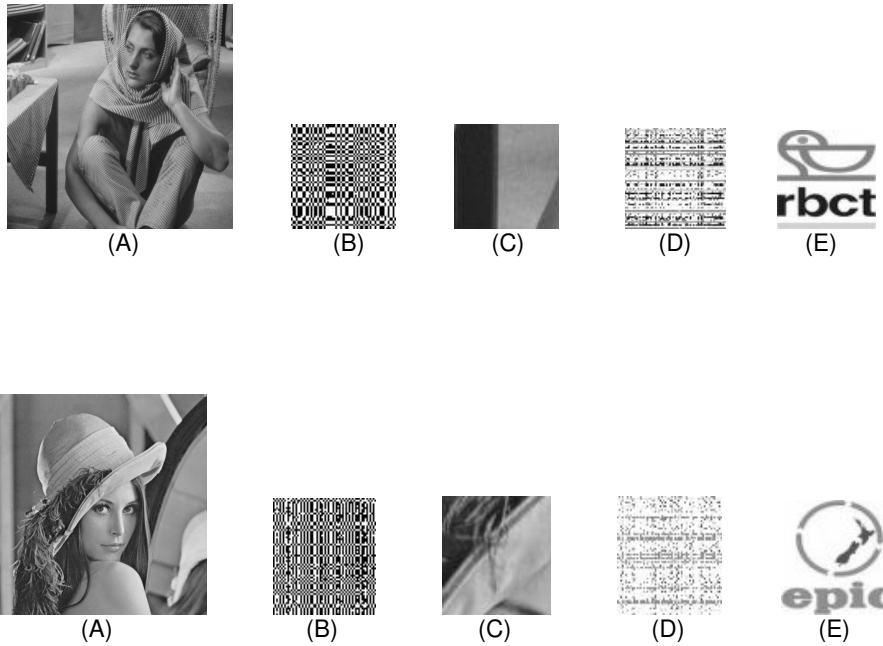

(E)



(A) (B) (C) (D) (E)

(A) (B) (C) (D) (E)

FIGURE: 2 Intermediate results of PSCV construction
A - Primary Image(512 * 512) , B - Patent Image(64 * 64) , C -Sub primary Image(64 * 64)
D - Shuffled Patent Image (IS) (64 * 64) , E - Projected Image(64 * 64).



(A) (B) (C) (D) (E)

(A) (B) (C) (D) (E)

(A) (B) (C) (D) (E)

FIGURE: 3 Intermediate results of Patent Image Reconstruction
A - Primary Image (512 * 512) , B - Projected Image(64 * 64)., C -Sub primary Image(64 * 64)
D - Shuffled Patent Image (IS) (64 * 64) , E - Patent Image(64 * 64)

4. CONCLUSION

In this paper, in part, we overviewed scores of issues that have been addressed for data encryption and watermarking in a DRM given the thrust toward security for emerging resource constrained DRM applications. We proposed a new solution that provides a better compromise between security and quality of an image. In this current solution we proposed the five level securities, which can defend the data from hack. This is resulting in a paradigm shift in the area of information protection, in which ideas from areas such as media processing are often incorporated to provide more lightweight solutions.

5. REFERENCES

1. "*Digital watermarking*" definition from http://en.wikipedia.org/wiki/ Digital_ watermarking

2. "*A Digital Watermarking System for Multimedia Copyright Protection*" - .Jian Zhao Fraunhofer Center for Research in Computer Graphics, Eckhard Koch Fraunhofer Institute for Computer Graphics, Wilhelminenstr. 7, D-64283 Darmstadt, Germany.

3. Power Point Presentation in *"Watermarking of Digital Images* "– by Assoc Prof. Dr. Aziza A. Manaf & Akram M. Zeki , 1st ENGAGE European Union - Southeast Asia ICT , Research Collaboration Conference, March 29–31, 2006

4. "*Shuffling Technique*" from - http://en.wikipedia.org/wiki/Shuffling.

5. Rahul Shukla, Pier Luigi Dragotti, Minh Do_, and Martin Vetterli "*Improved Quadtree Algorithm Based on Joint Coding for piecewise Smooth Image Compression*"

6. Raphael Finkel and J.L.Bentley (1974). "*Quad Trees: A Data Structure for Retrieval on Composite Keys*". Acta Informatica 4 (1): 1-9.

7. P. Strobach "*Quadtree structured recursive plane decomposition coding of images*", IEEE Trans. Signal Proc., vol. 39, pp. 1380-1397, June 1991.

8. *"AES Encryption Information*" - http://www.bitzipper.com/aes-encryption.html.

9. Announcing the "*ADVANCED ENCRYPTION STANDARD (AES)*" - Federal Information, Processing Standards Publication 197,November 26, 2001.

10. H. K. C. Chang, P. M. Chen, and L. L. Cheng, "*Overlapping Representation of Similar Images Using Linear Quadtrees Codes*," In 8th IPPR Conference on Computer Vision, Graphics and Image Processing, Tao-Yuang, Taiwan, R.O.C., Aug. 1995.

11. T. W. Lin, "*Compressed Quadtree Representations for Storing Similar Images*," Image and Vision Computing, Vol. 15, 1997, pp. 883-843.

12. F. Boland, J. O. Ruanaidh, and C. Dautzenberg, "*Watermarking digital images for copyright protection*," in Proc. IEEE Int. Conf. Image Proc. Applicat., 1995, pp. 321–326.

13. Ji-Hong Chang and Long-Wen Chang," *A New Image Copyright Protection Algorithm Using Digital Signature of Trading Message and Bar Code watermark*" palmerston North, November 2003

14. Hans Georg Schaathun," *On watermarking/fingerprinting for copyright protection*".

15. Soroosh Rezazadeh, and Mehran Yazdi," *A Nonoblivious Image Watermarking System Based on Singular Value Decomposition and Texture Segmentation*" PROCEEDINGS OF WORLD ACADEMY OF SCIENCE, ENGINEERING AND TECHNOLOGY VOLUME 13 MAY 2006 ISSN 1307-6884

16. JUAN R. HERNA´ NDEZ, FERNANDO PE´REZ-GONZA´ LEZ," *Statistical Analysis of Watermarking Schemes for Copyright Protection of Images*" PROCEEDINGS OF THE IEEE, VOL. 87, NO. 7, JULY 1999.

17. M. Barnia, F. Bartolinib, V. Cappellinib, E. Maglic, G. Olmo," *Near-lossless digital watermarking for copyright protection of remote sensing images*".

18. Md. Mahfuzur Rahman and Koichi Harada," *Parity enhanced topology based spot area watermarking method for copyright protection of layered 3D triangular mesh data*" IJCSNS International Journal of Computer Science and Network Security, VOL.6 No.2A, February 2006.

19. Nizar Sakr, Nicolas Georganas, and Jiying Zhao," *Copyright Protection of Image Learning Objects using Wavelet-based Watermarking and Fuzzy Logic*" 3rd annual e-learning conference on Intelligent Interactive Learning Object Repositories Montreal, Quebec, Canada, 9–11 November, 2006

20. Jacob Löfvenberg, Niclas Wiberg," *Random Codes for Digital Fingerprinting*".